

Description

METHOD AND SYSTEM FOR TRACKING USER PERFORMANCE

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This invention is a continuation in part of U.S. Serial No. 10/340,352 filed on January 10, 2003 and entitled SYSTEM AND METHOD FOR INCENTING PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS. The '352 application itself claims priority to U.S. Patent Application No. 10/192,488, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed on July 9, 2002 (which itself claims priority to U.S. Provisional No. 60/304,216 filed on July 10, 2001); U.S. Patent Application No. 10/318,432, entitled "SYSTEM AND METHOD FOR SELECTING LOAD OPTIONS FOR USE IN RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed December 13, 2002; U.S. Patent Application

No. 10/318,480, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed December 13, 2002; and, U.S. Provisional Patent Application No. 60/396,577 filed July 16, 2002. All of the above applications are hereby incorporated by reference.

FIELD OF INVENTION

[0002] This invention generally relates to tracking resource performance, and more particularly, to tracking the performance of resources using Radio Frequency Identification (RFID) in contact and contactless environments.

BACKGROUND OF INVENTION

[0003] A variety of hardware and software applications exist which, in a limited way, allow companies to keep track of resource performance. For example, many systems exist wherein a resource (e.g., employee) manually enters in the time spent on a task on a time card or a similar reporting device. However, there is a need for coordinating time card and task reporting with project planning. Microsoft Project® is a software application that allows companies to plan and track projects in order to increase business performance and efficiency. However, most project/resource

management tools require a resource to manually enter and plan a project. For example, the resource must often decide a project's scope, the kind of tasks associated with the project, the number of resources needed, and the availability of resources. Many times, the decisions are not accurate because a resource often attempts to merely predict the scope of these items. Further, if problems develop along the way, the resource typically must reschedule and try to account for the problems. Moreover, most project/resource management tools do not combine time entry with resource and task planning. Thus, a manager may assume that a resource is logging eight hours a day on a task, but in reality, the resource may only be logging five hours.

[0004] Additionally, the available project/resource management tools do not generally provide for grading or scoring of resources and/or resource efficiencies. It may be difficult, therefore, to plan the effectiveness of different resources. For example, a senior engineer may be more efficient and effective at a given task than an entry-level engineer. Further, because of the global aspect of many businesses, certain managers monitor resources located in remote places. However, most project/management tools do not

offer standard criteria for grading and tracking resources to assist in remote management. Further, many project/management tools do not provide sufficient capabilities for matching a resource to tasks most-suited to the resource's skill levels.

[0005] Manual entry and project management can lead to inaccuracies in reporting and planning. While other systems exist where a resource and/or manager can interface with a software application to track progress on a task, report time, and/or project plan, these software applications still require manual interfacing. Thus, a method for instantaneous and automatic task reporting, performance tracking and project planning is desired.

[0006] In terms of automation, companies are increasingly embodying RFID data acquisition technology in a fob, token or tag for use in completing transactions. A typical fob includes a transponder and is ordinarily a self-contained device which may be contained on any portable form factor. In some instances, a battery may be included with the fob to power the transponder. In which case the internal circuitry of the fob (including the transponder) may draw its operating power from the battery power source. Alternatively, the fob may exist independent of an internal

power source. In this instance the internal circuitry of the fob (including the transponder) may gain its operating power directly from an RF interrogation signal. U.S. Patent No. 5,053,774 issued to Schuermann describes a typical transponder RF interrogation system which may be found in the prior art. The Schuermann patent describes in general the powering technology surrounding conventional transponder structures. U.S. Patent No. 4,739,328 discusses a method by which a conventional transponder may respond to a RF interrogation signal. Other typical modulation techniques which may be used include, for example, ISO/IEC 14443 and the like.

[0007] One of the more visible uses of the RFID technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products. These products use transponders placed in a fob or tag which enables automatic identification of the resource when the fob is presented at a Point of Sale (POI) device. Fob identification data is typically passed to a third party server database, where the identification data is referenced to a resource (e.g., resource) credit or debit account. In an exemplary processing method, the server seeks authorization for the transaction by passing the transaction and account data to

an authorizing entity. Once authorization is received by the server, clearance is sent to the point of sale device for completion of the transaction. In this way, the conventional transaction processing method involves an indirect path which causes undue overhead due to the use of the third-party server. As such, a RFID system which includes instantaneous and automatic task reporting, performance tracking and project planning is desired.

SUMMARY OF INVENTION

[0008] A system and method for facilitating the use of RFID technology to track resource performance and task completion is disclosed. The transponder-reader system described herein may include a RFID reader operable to provide a RF interrogation signal for powering a transponder system, receiving a transponder system RF signal, and providing transponder system account data relative to the transponder system RF signal. The transponder-reader system may include a RFID protocol/sequence controller in electrical communication with one or more interrogators for providing an interrogation signal to a transponder, a RFID authentication circuit for authenticating the signal received from the transponder, a serial or parallel interface for interfacing with a point of interaction terminal, and an USB

or serial interface for use in personalizing the RFID reader and/or the transponder. The transponder-reader system may further include a fob including one or more transponders (e.g., modules) responsive to one or more interrogation signals and for providing an authentication signal for verifying that the transponder and/or the RFID reader are authorized to operate within the transponder-reader system. In this way, the fob may be responsive to multiple interrogation signals provided at different frequencies. Further, the fob may include a USB or serial interface for use with a computer network or with the RFID reader.

[0009] The RFID system and method according to the present invention may include a transponder which may be embodied in a fob, tag, card or any other form factor (e.g., wristwatch, keychain, cell phone, etc.), which may be capable of being presented for interrogation. In that regard, although the transponder is described herein as embodied in a fob, the invention is not so limited.

[0010] The system may further include a RFID reader configured to send a standing RFID recognition signal which may be transmitted from the RFID reader via radio frequency (or electromagnetic) propagation. The fob may be placed

within proximity to the RFID reader such that the RFID signal may interrogate the fob and initialize fob identification procedures.

[0011] In one exemplary embodiment, as a part of the identification process, the fob and the RFID reader may engage in mutual authentication. The RFID reader may identify the fob as including an authorized system transponder for receiving encrypted information and storing the information on the fob memory. Similarly, the fob, upon interrogation by the RFID reader, may identify the RFID reader as authorized to receive the encrypted and stored information. Where the RFID reader and the fob successfully mutually authenticate, the fob may transmit to the RFID reader certain information identifying the resource's performance tracking account or accounts to which the fob is associated. The RFID reader may receive the information and forward the information to facilitate performance tracking. In one exemplary embodiment, the RFID reader may forward the information to a point of interaction terminal (e.g., POI or computer interface) for transaction completion.

[0012] In another exemplary embodiment, the fob completes tasks via a computer interface. The fob may be connected

to the computer using a USB or serial interface fob account information may be transferred to the computer for use in tracking a resource's performance via a network (e.g., the Internet).

[0013] In still another exemplary embodiment of the invention, a system is disclosed which enables the fob resource and/or a manager access to a resource engine, wherein the resource engine may be used to automatically grade, track, score, and assign resources based on resource skills and skill sets.

[0014] These features and other advantages of the system and method, as well as the structure and operation of various exemplary embodiments of the system and method, are described below.

BRIEF DESCRIPTION OF DRAWINGS

[0015] The accompanying drawings, wherein like numerals depict like elements, illustrate exemplary embodiments of the present invention, and together with the description, serve to explain the principles of the invention. In the drawings:

[0016] FIG. 1A illustrates an exemplary RFID-based system in accordance with the present invention, wherein exemplary components used for fob performance tracking are depicted;

- [0017] FIG. 1B illustrates an exemplary personalization system in accordance with the present invention;
- [0018] FIG. 2 is a schematic illustration of an exemplary fob in accordance with the present invention;
- [0019] FIG. 3 is a schematic illustration of an exemplary RFID reader in accordance with the present invention;
- [0020] FIG. 4 is an exemplary flow diagram of an exemplary authentication process in accordance with the present invention;
- [0021] FIG. 5 is an exemplary flow diagram of an exemplary decision process for a protocol/sequence controller in accordance with the present invention;
- [0022] FIGS. 6A–B are an exemplary flow diagram of a fob personalization process in accordance with the present invention;
- [0023] FIGS. 7A–B are an exemplary flow diagram of a RFID reader personalization process in accordance with the present invention;
- [0024] FIG. 8 is a flow diagram of an exemplary performance tracking process in accordance with the present invention;
- [0025] FIG. 9 is another schematic illustration of an exemplary fob configured to facilitate biometric security devices in accordance with the present invention;

- [0026] FIG. 10 includes a flowchart illustrating an exemplary resource engine system configured to facilitate tracking of resource performance;
- [0027] FIG. 11 includes an exemplary block diagram illustrating additional details of the resource engine component of the present invention;
- [0028] FIG. 12 includes a flowchart illustrating an exemplary method for assigning tasks in accordance with the present invention; and
- [0029] FIG. 13 includes an exemplary screen shot of a software program used to facilitate tracking of resource performance in accordance with the present invention.

DETAILED DESCRIPTION

- [0030] The detailed description of exemplary embodiments of the invention herein makes reference to the accompanying block diagrams and flowcharts, which show the exemplary embodiment by way of illustration and its best mode. While these exemplary embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the invention. Thus, the detailed description

herein is presented for purposes of illustration only and not of limitation. For example, the steps recited in any of the method or process descriptions may be executed in any order and are not limited to the order presented.

[0031] Moreover, it should be appreciated that the particular implementations shown and described herein are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, certain sub-components of the individual operating components, conventional data networking, application development and other functional aspects of the systems may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical system.

[0032] The present invention may be described herein in terms of block diagrams, screen shots and flowcharts, optional selections and various processing steps. Such functional blocks may be realized by any number of hardware and/or

software components configured to perform to specified functions. For example, the present invention may employ various integrated circuit components (e.g., memory elements, processing elements, logic elements, look-up tables, and the like), which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, extensible markup language (XML), JavaCard and MULTOS with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction on cryptography, review a text written by Bruce Schneier entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons (second edition, 1996), herein incorporated by reference.

[0033] In addition, many applications of the present invention could be formulated. The exemplary network disclosed

herein may include any system for exchanging data or tracking resource performance, such as a distributed system, a thin cable network, an Ethernet, a token ring network, the internet, an intranet, an extranet, wide area network (WAN), local area network (LAN), satellite communications, and/or the like. It is noted that the network may be implemented as other types of networks, such as an interactive television network (ITN).

[0034] The system user/resource may interact with the system via any input device such as, a keypad, keyboard, mouse, kiosk, personal digital assistant, handheld computer (e.g., Palm Pilot®, Blueberry®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, work station, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris or the like. Moreover, although the invention may frequently be described as being implemented with TCP/IP communications protocol, it should be understood that the invention could also be implemented using SNA, IPX, Appletalk, IPte, NetBIOS, OSI or any number of communications protocols.

Moreover, the system contemplates, the use, sale, or distribution of any goods, services or information over any network having similar functionality described herein.

[0035] FIG. 1A illustrates an exemplary RFID performance tracking transaction system 100A in accordance with the present invention, wherein exemplary components for use in completing a fob transaction are depicted. In general, the operation of system 100A may begin when a fob 102 is presented for tracking a resource's performance, and is interrogated by an RFID reader 104 or, alternatively, a computer interface (e.g., user interface) 134. Fob 102 and RFID reader 104 may then engage in mutual authentication after which the transponder 114 may provide the transponder identification and/or account identifier to RFID reader 104 which may further provide the information to a resource engine 130 via a point of interaction terminal 110. For further information related to tracking and optimizing resources, see, for example, U.S. Patent Application No. 10/770,684 filed February 3, 2004, and entitled "SYSTEM AND METHOD FOR RESOURCE OPTIMIZATION", which is hereby incorporated by reference.

[0036] As used herein, a resource may include any user, person, employee, employer officer, entity, manager, business,

client, corporation, customer, contractor, administrator, operator, equipment, supply, package, machinery, hardware and/or software. Employer, as used herein, may include any performance tracking entity, manager, controller, administrator, operator and/or company.

[0037] The term tracking as used herein, may include any management, assignment, grading, scoring, manipulation, tracking, control, allocation, and/or any other modification to application information, resource information, skills information, and/or task information. Tasks may include shipments, assignments, problem tickets, enhancements, analyses, builds, designs, components, assemblies, and/or any other projects.

[0038] Resource engine 130 may be a stand-alone system or incorporated into any pre-existing network or metrics system via any software and/or hardware customization or upgrades. Resource engine 130 may include any hardware and/or software discussed herein. Resource engine 130 may include a host server or other computing systems including a processor for processing digital data, a memory coupled to said processor for storing digital data, an input digitizer coupled to the processor for inputting digital data, an application program stored in said memory and

accessible by said processor for directing processing of digital data by said processor, a display coupled to the processor and memory for displaying information derived from digital data processed by said processor and a plurality of databases, said databases including resource data, application data, skill data, category data and/or like data that could be used in association with the present invention. As those skilled in the art will appreciate, resource engine 130 computer will typically include an operating system (e.g., Windows NT, 95/98/2000, Linux, Solaris, etc.) as well as various conventional support software and drivers typically associated with computers.

[0039] Resource engine 130 may also be used in conjunction with any monitoring system, hardware or software, configured to monitor, manage and track systems within resource engine 130. One example of such monitoring system is an off-the-shelf program such as IBM's Tivoli NetView®, which automatically detects problems and responds to those problems at a local level. For example, NetView may detect a problem with an application and generate an information management record (IMR) in conjunction with that problem. The IMR from the monitoring system may then be transmitted to resource engine 130

through any of the communications networks described herein.

[0040] Similarly, resource engine 130 may include, or be used in conjunction with, any type of personal computer, network computer, workstation, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris or the like. Moreover, the invention may be implemented using TCP/IP communications protocols, IPX, Appletalk, IP-6, NetBIOS, OSI or any number of existing or future protocols. Resource engine 130 will be discussed in greater detail herein.

[0041] System 100A may include fob 102 having a transponder 114 and RFID reader 104 in RF communication with fob 102. Although the present invention is described with respect to fob 102, the invention is not to be so limited. Indeed, system 100A may include any device having a transponder which is configured to communicate with RFID reader 104 via RF communication. Typical devices may include, for example, a key ring, tag, card, cell phone, wristwatch or any such form capable of being presented for interrogation.

[0042] RFID reader 104 may be configured to communicate using an RFID internal antenna 106. Alternatively, RFID reader 104 may include an external antenna 108 for communications with fob 102, where the external antenna may be made remote to RFID reader 104 using a suitable cable and/or data link 120. RFID reader 104 may be further in communication with resource engine 130 via a data link 122. System 100A may include a transaction completion system including a point of interaction device such as, for example, employer point of interaction terminal 110 or computer 134. In one exemplary embodiment the transaction completion system may include resource engine 130 and/or point of interaction terminal 110 in communication with RFID reader 104 (via data link 122). As described more fully below, the transaction completion system may include computer 134 connected to a network 136 and to transponder 114 via a USB connector 132.

[0043] Although the point of interaction (POI) is described herein with respect to a resource POI terminal, the invention is not to be so limited. Indeed, a POI terminal is used herein by way of example, and the POI may be any device capable of receiving fob account data. In this regard, the POI may be any point of interaction device and/or terminal

enabling the resource to complete a performance tracking transaction using fob 102. POI terminal 110 may be in further communication with a user interface 118 (via data link 128) for providing a resource and/or manager access to resource engine 130 information. In addition, POI terminal 110 may be in communication with an employer host network 112 (via data link 124) for processing any tracking request. In this arrangement, information provided by RFID reader 104 is provided to POI terminal 110 of resource engine 130 via data link 122. POI terminal 110 may receive the information (and alternatively may receive any identity verifying information from user interface 118 via data link 128) and provide the information to host network 112 for processing.

[0044] A variety of conventional communications media and protocols may be used for data links 120, 122, 124, and 128 as well as for any other communication links mentioned herein. For example, data links 120, 122, 124, and 128 may be an Internet Service Provider (ISP) configured to facilitate communications over a local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Lines (DSL), or any wireless communication media. In ad-

dition, resource engine 130, including POI terminal 110 and host network 112, may reside on a local area network which interfaces to a remote network (not shown) for remote authorization of an intended performance tracking transaction. Host network 112 may be an employer network, such as an employer LAN, WAN and/or intranet. Resource engine 130 may communicate with the remote network via a leased line, such as a T1, D3 line, or the like. Such communications lines are described in a variety of texts, such as, "Understanding Data Communications," by Gilbert Held, which is incorporated herein by reference.

[0045] A transponder and/or account identifier, as used herein, may include any number or identifier for an account (e.g., any device, code, or other identifier/indicia suitably configured to allow a resource to interact or communicate with system 100A, such as, for example, authorization/access code, personal identification number (PIN), Internet code, digital certificate, biometric data, and/or other identification indicia). A transponder identifier may be further coordinated with fob 102 as well as a resource identifier. For example, a resource may have a resource account identifier associated with him. The resource may also carry fob 102, which can only be used by that specific

resource. Fob 102, in turn has a unique transponder identifier such that the transponder identifier may be associated with both the specific fob 102 and the resource holding fob 102.

[0046] Resource engine 130 may also have one or more employer account identifiers associated with it. An employer account identifier may be used by an employer to associate a resource and/or fob 102 with a specific employer account. For example, the employer account identifiers may be used to track a resource's performance on different tasks associated with the employer accounts.

[0047] The transponder identifier may be maintained by a performance tracking provider (e.g., employer) and which may be used to track a resource's performance. A typical transponder identifier (e.g., account data) may be correlated to a resource number, identifier, etc. For ease in understanding, the present invention may be described with respect to a resource ID. However, it should be noted that the invention is not so limited and other accounts permitting an exchange of information for an account data value is contemplated to be within the scope of the present invention.

[0048] The transponder identifier may be distributed and stored

in any form of plastic, electronic, magnetic, and/or optical device capable of transmitting or downloading data to a second device. A resource account identifier may be, for example, a resource's ten-digit social security number. The resource account identifier may also be, for example, the number of the resource's company credit card. In one exemplary embodiment, the transponder and/or resource account identifier may include a unique fob serial number and resource identification number, as well as specific application applets. The transponder and/or resource account identifiers may be stored in fob 102 inside a database 214, as described more fully below. Database 214 may be configured to store multiple account identifiers issued to fob 102 resources by the same or different account providing institutions.

[0049] FIG. 2 illustrates the many functions of exemplary fob 102 in accordance with the present invention. Fob 102 may be an RFID fob which may be presented by the resource to facilitate an exchange of information, for tracking a resource's performance on one or more tasks. As described herein, by way of example, fob 102 may be an RFID fob which may be presented for facilitating tracking resource performance.

[0050] Fob 102 may include an antenna 202 for receiving an interrogation signal from RFID reader 104 via antenna 106 (or alternatively, via external antenna 108). Fob antenna 202 may be in communication with transponder 114. In one exemplary embodiment, transponder 114 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 202 may be of the 13 MHz variety. The transponder 114 may be in communication with a transponder compatible modulator/demodulator 206 configured to receive the signal from transponder 114 and configured to modulate the signal into a format readable by any later connected circuitry. Further, modulator/demodulator 206 may be configured to format (e.g., demodulate) a signal received from the later connected circuitry in a format compatible with transponder 114 for transmitting to RFID reader 104 via antenna 202. For example, where transponder 114 is of the 13.56 MHz variety, modulator/demodulator 206 may be ISO/IEC 14443-2 compliant.

[0051] Modulator/demodulator 206 may be coupled to a protocol/sequence controller 208 for facilitating control of the authentication of the signal provided by RFID reader 104, and for facilitating control of the sending of fob 102

transponder identifier. In this regard, protocol/sequence controller 208 may be any suitable digital or logic driven circuitry capable of facilitating determination of the sequence of operation for fob 102 inner-circuitry. For example, protocol/sequence controller 208 may be configured to determine whether the signal provided by RFID reader 104 is authenticated, and thereby providing to RFID reader 104 the account identifier stored on fob 102.

[0052] Protocol/sequence controller 208 may be further in communication with authentication circuitry 210 for facilitating authentication of the signal provided by RFID reader 104. Authentication circuitry may be further in communication with a non-volatile secure memory database 212. Secure memory database 212 may be any suitable elementary file system such as that defined by ISO/IEC 7816-4 or any other elementary file system allowing a lookup of data to be interpreted by the application on the chip.

[0053] The data may be used by protocol/sequence controller 208 for data analysis and used for management and control purposes, as well as security purposes. Authentication circuitry may authenticate the signal provided by RFID reader 104 by association of the RFID signal to authenti-

cation keys stored on database 212. Encryption circuitry may use keys stored on database 212 to perform encryption and/or decryption of signals sent to or from RFID reader 104.

[0054] In addition, protocol/sequence controller 208 may be in communication with a database 214 for storing at least fob 102 transponder account data, and a unique fob 102 identification code. Protocol/sequence controller 208 may be configured to retrieve the account identifier from database 214 as desired. Database 214 may be of the same configuration as database 212 described above. The fob transponder account data and/or unique fob identification code stored on database 214 may be encrypted prior to storage. Thus, where protocol/sequence controller 208 retrieves the account data, and or unique fob identification code from database 214, the transponder account identifier may be encrypted when being provided to RFID reader 104. Further, the data stored on database 214 may include, for example, an unencrypted unique fob 102 identification code, a resource identification, Track 1 and 2 data, as well as specific application applets.

[0055] Database 212 and any other database discussed herein may be any type of database, such as relational, hierarchi-

cal, graphical, object-oriented, and/or other database configurations. Common database products that may be used to implement the databases include DB2 by IBM (White Plains, New York), various database products available from Oracle Corporation (Redwood Shores, California), Microsoft Access or Microsoft SQL Server by Microsoft Corporation (Redmond, Washington), or any other suitable database product. Moreover, the databases may be organized in any suitable manner, for example, as data tables or lookup tables. Each record may be a single file, a series of files, a linked series of data fields or any other data structure. Association of certain data may be accomplished through any desired data association technique such as those known or practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in pre-selected databases or data sectors.

[0056] More particularly, a "key field" partitions the database according to the high-level class of objects defined by the

key field. For example, certain types of data may be designated as a key field in a plurality of related data tables and the data tables may then be linked on the basis of the type of data in the key field. In this regard, the data corresponding to the key field in each of the linked data tables may be preferably the same or of the same type. However, data tables having similar, though not identical, data in the key fields may also be linked by using AGREP, for example. In accordance with one aspect of the present invention, any suitable data storage technique may be utilized to store data without a standard format. Data sets may be stored using any suitable technique, for example, storing individual files using an ISO/IEC 7816-4 file structure; implementing a domain whereby a dedicated file may be selected that exposes one or more elementary files containing one or more data sets; using data sets stored in individual files using a hierarchical filing system; data sets stored as records in a single file (for example, compression, SQL accessible, hashed via one or more keys, numeric, alphabetical by first tuple, etc.); block of binary (BLOB); stored as ungrouped data elements encoded using ISO/IEC 7816-6 data elements; stored as ungrouped data elements encoded using ISO/IEC Abstract

Syntax Notation (ASN.1) as in ISO/IEC 8824 and 8825; and/or other proprietary techniques that may include fractal compression methods, image compression methods, etc.

[0057] In one exemplary embodiment, the ability to store a wide variety of information in different formats may be facilitated by storing the information as a Block of Binary (BLOB). Thus, any binary information may be stored in a storage space associated with a data set. The BLOB method may store data sets as ungrouped data elements formatted as a block of binary via a fixed memory offset using either fixed storage allocation, circular queue techniques, or best practices with respect to memory management (e.g., paged memory, least recently used, etc.). By using BLOB methods, the ability to store various data sets that have different formats facilitates the storage of data associated with a wide variety of system components by multiple and unrelated owners of the data sets. For example, a first data set which may be stored may be provided by a first issuer, a second data set which may be stored may be provided by an unrelated second issuer, and yet a third data set which may be stored, may be provided by a third issuer unrelated to the first and second issuer. Each

of these three exemplary data sets may contain different information that may be stored using different data storage formats and/or techniques. Further, each data set may contain subsets of data which also may be distinct from other subsets.

[0058] As stated above, in various embodiments of the present invention, the data may be stored without regard to a common format. However, in one exemplary embodiment of the present invention, the data set (e.g., BLOB) may be annotated in a standard manner when provided for manipulating the data onto the network. The annotation may comprise a short header, trailer, or other appropriate indicator related to each data set that may be configured to convey information useful in managing the various data sets. For example, the annotation may be called a "condition header," "header," "trailer," or "status," herein, and may comprise an indication of the status of the data set or may include an identifier correlated to a specific issuer or owner of the data. In one example, the first three bytes of each data set BLOB may be configured or configurable to indicate the status of that particular data set (e.g., LOADED, INITIALIZED, READY, BLOCKED, REMOVABLE, or DELETED). Subsequent bytes of data may be used to indi-

cate for example, the identity of the resource, user, account identifier or the like. Each of these condition annotations are further discussed herein.

[0059] With reference again to the exemplary block diagrams illustrated in FIG's. 1 and 2, fob 102 may be configured to respond to multiple interrogation frequency transmissions provided by RFID reader 104. That is, as described more fully below, RFID reader 104 may provide more than one RF interrogation signal. In this case, fob 102 may be configured to respond to the multiple frequencies by including in fob 102 one or more additional RF signal receiving/transmitting units 226. RF signal receiving/transmitting unit 226 may include an antenna 218 and transponder 220 where antenna 218 and transponder 220 are compatible with at least one of the additional RF signals provided by RFID reader 104. For example, in one exemplary embodiment, fob 102 may include a 134 KHz antenna 218 configured to communicate with a 134 KHz transponder 220. In this exemplary configuration, an ISO/IEC 14443-2 compliant modulator/demodulator may not be required. Instead, the 134 KHz transponder may be configured to communicate directly with the protocol/sequence controller 208 for transmission and receipt of authentication

and account identifier signals as described above.

[0060] In another embodiment, fob 102 may further include a universal serial bus (USB) connector 132 for interfacing fob 102 to user interface 134. User interface 134 may be further in communication with POI terminal 110 via a network 136. Network 136 may be the Internet, an intranet, or the like as is described above with respect to network 112. Further, user interface 134 may be similar in construction to any conventional input devices and/or computing systems aforementioned for permitting a resource to interact with network 136 and/or resource engine 130 through user interface 134. In one exemplary embodiment, fob 102 may be configured to facilitate online performance tracking. A USB converter 222 may be in communication with a USB connector 232 for facilitating the transfer of information between the modulator/demodulator 206 and USB connector 132. Alternatively, USB converter 222 may be in communication with protocol/sequence controller 208 to facilitate the transfer of information between protocol/sequence controller 208 and USB connector 132.

[0061] Where fob 102 includes USB connector 132, fob 102 may be in communication with, for example, a USB port on

user interface 134. The information retrieved from fob 102 may be compatible with employee badge and/or smart card technology enabling usage of interactive applications on the Internet. No RFID reader may be required in this embodiment since the connection to POI terminal 110 may be made using a USB port on user interface 134 and network 136.

[0062] Fob 102 may include means for enabling activation of the fob by the resource. In one exemplary embodiment, a switch 230 which may be operated by the user/resource of fob 102. Switch 230 on fob 102 may be used to selectively or inclusively activate fob 102 for particular uses. In this context, the term "selectively" may mean that switch 230 enables the resource to place fob 102 in a particular operational mode. For example, the resource may place fob 102 in a mode for enabling tracking the resource's performance of a specific task using a selected task number. Alternatively, the fob may be placed in a mode as such that the fob account identifier is provided by USB port 132 (or serial port) only and fob transponder 114 is disabled. In addition, the term "inclusively" may mean that fob 102 is placed in an operational mode permitting fob 102 to be responsive to the RF interrogation and interro-

gation via the USB connector 132. In one particular embodiment, switch 230 may remain in an OFF position ensuring that one or more applications or accounts associated with fob 102 are non-reactive to any commands issued by RFID reader 104. As used herein, the OFF position may be termed the "normal" position of the activation switch 230, although other normal positions are contemplated.

[0063] In another exemplary embodiment, when switch 230 is moved from the OFF position, fob 102 may be deemed activated by the resource. That is, switch 230 may activate internal circuitry in fob 102 for permitting the fob to be responsive to RF signals (e.g., commands from RFID reader 104). In this way, switch 230 may facilitate control of the active and inactive states of fob 102. Such control increases the system security by preventing inadvertent or illegal use of fob 102.

[0064] In one exemplary embodiment, switch 230 may be a simple mechanical device in communication with circuitry which may electrically prevent the fob from being powered by a RFID reader. That is, when switch 230 is in its normal position, switch 230 may provide a short to fob 102 internal circuitry, preventing fob 102 from being re-

sponsive to interrogation by RF or via the USB connector 230. In this arrangement, switch 230 may be, for example, a "normally closed" (NC) configured switch, which may be electrically connected to antenna 202 at the interface of antenna 202 and transponder 114. Switch 230 may be depressed, which may open switch 230 fully activating antenna 202.

[0065] In yet another exemplary embodiment, fob 102 may include a biometric sensor and biometric membrane configured to operate as switch 230 and activate fob 102 when provided with a biometric signal from a authorized resource using fob 102. Such biometric signal may be the digital reading of a fingerprint, thumbprint, or the like. Typically, where biometric circuitry is used, the biometric circuitry may be powered by an internal voltage source (e.g., battery). In this case, the switch may not be a simple mechanical device, but a switch which is powered. In yet another exemplary embodiment, switch 230 may be battery powered though no biometric circuitry is present in fob 102.

[0066] In yet another embodiment, switch 230 may be a logic switch. Where switch 230 is a logic switch, switch 230 control software may be read from the sequence con-

troller 208 to selectively control the activation of the various fob 102 components.

[0067] FIG. 3 illustrates an exemplary block diagram of RFID reader 104 in accordance with an exemplary embodiment of the present invention. RFID reader 104 includes, for example, an antenna 106 coupled to a RF module 302, which is further coupled to a control module 304. In addition, RFID reader 104 may include antenna 108 positioned remotely from RFID reader 104 and coupled to RFID reader 104 via a suitable cable 120, or other wire or wireless connection.

[0068] RF module 302 and antenna 106 may be suitably configured to facilitate communication with fob 102. Where fob 102 is formatted to receive a signal at a particular RF frequency, RF module 302 may be configured to provide an interrogation signal at that same frequency. For example, in one exemplary embodiment, fob 102 may be configured to respond to an interrogation signal of about 13.56 MHz. In this case, RFID antenna 106 may be 13 MHz and may be configured to transmit an interrogation signal of about 13.56 MHz. That is, fob 102 may be configured to include a first and second RF module (e.g., transponder) where the first module may operate using a 134 kHz fre-

quency and the second RF module may operate using a 13.56 MHz frequency. RFID reader 104 may include two receivers which may operate using the 134 kHz frequency, the 13.56 MHz frequency or both. When RFID reader 104 is operating at 134 kHz frequency, only operation with the 134 kHz module on fob 102 may be possible. When reader 104 is operating at the 13.56 MHz frequency, only operation with the 13.56 MHz module on fob 102 may be possible. Where RFID reader 104 supports both a 134 kHz frequency and a 13.56 MHz RF module, fob 102 may receive both signals from RFID reader 104. In this case, fob 102 may be configured to prioritize selection of the one or the other frequency and reject the remaining frequency. Alternatively, RFID reader 104 may receive signals at both frequencies from the fob upon interrogation. In this case, RFID reader 104 may be configured to prioritize selection of one or the other frequency and reject the remaining frequency.

[0069] Further, a protocol/sequence controller 314 may include an optional feedback function for notifying the resource of the status of a particular performance tracking transaction. For example, the optional feedback may be in the form of an LED, LED screen and/or other visual display

which is configured to light up or display a static, scrolling, flashing and/or other message and/or signal to inform a resource using fob 102 that a performance tracking transaction is initiated (e.g., fob is being interrogated), the fob is valid (e.g., fob is authenticated), a performance tracking transaction is being processed, (e.g., fob transponder account identifier is being read by RFID reader) and/or the transaction is accepted or denied (e.g., account identifiers approved or disapproved). Such an optional feedback may or may not be accompanied by an audible indicator (or may present the audible indicator singly) for informing fob 102 resource of the performance tracking transaction status. The audible feedback may be a simple tone, multiple tones, musical indicator, and/or voice indicator configured to signify when the fob 102 is being interrogated, the performance tracking transaction status, or the like.

[0070] RFID antenna 106 may be in communication with a transponder 306 for transmitting an interrogation signal and receiving at least one of an authentication request signal and/or an account data from fob 102. Transponder 306 may be of similar description as transponder 114 of FIG. 2. In particular, transponder 306 may be configured

to send and/or receive RF signals in a format compatible with antenna 106 in similar manner as was described with respect to fob transponder 114. For example, where transponder 306 is 13.56 MHz RF rated antenna 106 may be 13.56 MHz compatible. Similarly, where transponder 306 is ISO/IEC 14443 rated, antenna 106 may be ISO/IEC 14443 compatible.

[0071] RF module 302 may include, for example, transponder 306 in communication with authentication circuitry 308 which may be in communication with a secure database 310. Authentication circuitry 308 and database 310 may be of similar description and operation as described with respect to authentication circuitry 210 and secure memory database 212 of FIG. 2. For example, database 310 may store data corresponding to fob 102 which may be used to authorize the tracking of resource performance over system 100. Database 310 may additionally store RFID reader 104 identifying information and/or provide such information to fob 102 for use in authenticating whether RFID reader 104 is authorized to be provided the fob transponder account identifier stored on fob database 214.

[0072] Authentication circuitry 308 may be of similar description

and operation as authentication circuitry 210. That is, authentication circuitry 308 may be configured to authenticate the signal provided by fob 102 in a similar manner that authentication circuitry 210 may be configured to authenticate the signal provided by RFID reader 104. As is described more fully below, fob 102 and RFID reader 104 engage in mutual authentication. In this context, "mutual authentication" may mean that operation of the system 100 may not take place until fob 102 authenticates the signal from RFID reader 104, and RFID reader 104 authenticates the signal from fob 102.

[0073] FIG. 4 depicts a flowchart of an exemplary authentication process in accordance with the present invention. The authentication process is depicted as one-sided. That is, the flowchart depicts the process of RFID reader 104 authenticating fob 102, although similar steps may be followed in the instance that fob 102 authenticates RFID reader 104.

[0074] As noted, database 212 may store security keys for encrypting or decrypting signals received from RFID reader 104. In an exemplary authentication process, where RFID reader 104 is authenticating fob 102, RFID reader 104 may provide an interrogation signal to fob 102 (step 402).

The interrogation signal may include a random code generated by the RFID reader authentication circuit 210, which is provided to fob 102 and which is encrypted using an unique encryption key corresponding to the unique fob 102 identification code. For example, protocol/sequence controller 314 may provide a command to activate the authentication circuitry 308. Authentication circuitry 308 may provide from database 310 a fob interrogation signal including a random number as a part of the authentication code generated for each authentication signal. The authentication code may be an alphanumeric code which is recognizable (e.g., readable) by RFID reader 104 and fob 102. The authentication code may be provided to fob 102 via the RFID RF interface 306 and antenna 106 (or alternatively antenna 108).

[0075] Fob 102 receives the interrogation signal (step 404). The interrogation signal including the authorization code may be received at RF interface 114 via antenna 202. Once fob 102 is activated, the interrogation signal including the authorization code may be provided to the modulator/demodulator circuit 206 where the signal may be demodulated prior to providing the signal to protocol/sequence controller 208. Protocol/sequence controller 208 may rec-

ognize the interrogation signal as a request for authentication of fob 102, and provide the authentication code to authentication circuit 210. The fob 102 may then encrypt the authentication code (step 406). In particular, encryption may be done by authentication circuit 210, which may receive the authentication code and encrypt the code prior to providing the encrypted authentication code to protocol/sequence controller 208. Fob 102 may then provide the encrypted authentication code to RFID reader 104 (step 408). That is, the encrypted authentication code may be provided to RFID reader 104 via modulator/demodulator circuit 206, RF interface 114 (e.g., transponder 114) and antenna 106.

[0076] RFID reader 104 may then receive the encrypted authentication code and decrypt it (step 410). That is, the encrypted authentication code may be received at antenna 106 and RF interface 306 and may be provided to authentication circuit 308. Authentication circuit 308 may be provided a security authentication key (e.g., transponder system decryption key) from database 310. The authentication circuit may use the authentication key to decrypt (e.g., unlock) the encrypted authorization code. The authentication key may be provided to the authentication

circuit based on the unique fob 102 identification code. For example, the encrypted authentication code may be provided along with the unique fob 102 identification code. The authentication circuit may receive the unique fob 102 identification code and retrieve from database 310 a transponder system decryption key correlative to the unique fob 102 identification code for use in decrypting the encrypted authentication code.

[0077] Once the authentication code is decrypted, the decrypted authentication code is compared to the authentication code provided by RFID reader 104 at step 402 (step 412) to verify its authenticity. If the decrypted authorization code is not readable (e.g., recognizable) by the authentication circuit 308, fob 102 is deemed to be unauthorized (e.g., unverified) (step 418) and the operation of system 100 is terminated (step 420). Contrarily, if the decrypted authorization code is recognizable (e.g., verified) by fob 102, the decrypted authorization code is deemed to be authenticated (step 414), and the transaction is allowed to proceed (step 416). In one particular embodiment, the proceeding transaction may mean that fob 102 may authenticate RFID reader 104 prior to RFID reader 104 authenticating fob 102, although, it should be apparent that

RFID reader 104 may authenticate fob 102 prior to fob 102 authenticating RFID reader 104.

[0078] It should be noted that in an exemplary verification process, authorization circuit 308 may determine whether the unlocked authorization code is identical to the authorization code provided in step 402. If the codes are not identical then fob 102 is not authorized to access system 100. Although, the verification process is described with respect to identity, identity is not required. For example, authentication circuit 308 may verify the decrypted code through any protocol, steps, or process for determining whether the decrypted code corresponds to authorized fob 102.

[0079] Authentication circuitry 308 may additionally be in communication with protocol/sequence controller 314 of similar operation and description as protocol/sequence controller 208 of FIG. 2. That is, protocol/sequence device controller 314 may be configured to determine the order of operation of RFID reader 104 components. For example, FIG. 5 illustrates an exemplary decision process under which protocol/sequence controller 314 may operate. Protocol/sequence controller 314 may command the different components of RFID reader 104 based on whether

fob 102 is present (step 502). For example, if fob 102 is not present, then protocol/sequence controller 314 may command RFID reader 104 to provide an uninterrupted interrogation signal (step 504). That is, protocol/sequence controller 314 may command authentication circuit 308 to provide an uninterrupted interrogation signal until the presence of fob 102 is realized. If fob 102 is present, the protocol/sequence controller 314 may command RFID reader 104 to authenticate fob 102 (step 506).

[0080] As noted above, authentication may mean that protocol/sequence controller 314 may command authentication circuit 308 to provide fob 102 with an authorization code. If a response is received from fob 102, protocol/sequence controller may determine if the response is a response to RFID reader 104 provided authentication code, or if the response is a signal requiring authentication (step 508). If the signal requires authentication, then protocol/sequence controller 314 may activate the authentication circuit as described above (step 506). On the other hand, if fob 102 signal is a response to the provided authentication code, then protocol/sequence controller 314 may command RFID reader 104 to retrieve the appropriate security key for enabling recognition of the signal (step

510). That is, protocol/sequence controller 314 may command authentication circuit 308 to retrieve from database 310 a security key (e.g., transponder system decryption key), unlock the signal, and compare the signal to the signal provided by RFID reader 104 in the authentication process (e.g., step 506). If the signal is recognized, protocol/sequence controller 314 may determine that fob 102 is authorized to access system 100. If the signal is not recognized, then fob 102 is considered not authorized. In which case, protocol/sequence controller 314 may command the RFID controller to interrogate for authorized fobs (step 504).

[0081] Once protocol/sequence controller 314 determines that fob 102 is authorized, protocol/sequence controller 314 may seek to determine if additional signals are being sent by fob 102 (step 514). If no additional signal is provided by fob 102, then protocol/sequence controller 314 may provide all the components of RFID reader 104 to remain idle until such time as a signal is provided (step 516). Contrarily, where an additional fob 102 signal is provided, protocol/sequence controller 314 may determine if fob 102 is requesting access to resource engine 130 POI terminal 110 or if fob 102 is attempting to interrogate RFID

reader 104 for return (e.g., mutual) authorization (step 518). Where fob 102 is requesting access to resource engine 130 POI terminal 110, protocol/sequence controller 314 may command RFID reader 104 to open communications with POI terminal 110 (step 524). In particular, protocol/sequence controller 314 may command POI terminal communications interface 312 to become active, permitting transfer of data between RFID reader 104 and resource engine 130 POI terminal 110.

[0082] On the other hand, if protocol/sequence controller determines that fob 102 signal is a mutual interrogation signal, then protocol/sequence controller 314 may command RFID reader 104 to encrypt the signal (step 520). Protocol/sequence controller 314 may command encryption authentication circuit 318 to retrieve from database 320 the appropriate encryption key in response to fob 102 mutual interrogation signal. Protocol/sequence controller 314 may then command RFID reader 104 to provide the encrypted mutual interrogation signal to fob 102. Protocol/sequence controller 314 may command authentication circuit 318 to provide an encrypted mutual interrogation signal for fob 102 to mutually authenticate. Fob 102 may then receive the encrypted mutual interrogation signal

and retrieve from authentication circuitry 212 a RFID reader decryption key.

[0083] Although an exemplary decision process of protocol/sequence controller 314 is described, it should be understood that a similar decision process may be undertaken by protocol/sequence controller 208 in controlling the components of fob 102. Indeed, as described above, protocol/sequence controller 314 may have similar operation and design as protocol/sequence controller 208. In addition, to the above, protocol/sequence controllers 208 and 314 may incorporate in the decision process appropriate commands for enabling USB interfaces 222 and 316, when the corresponding device is so connected.

[0084] Encryption/decryption component 318 may be further in communication with a secure account identifier database 320 which stores the security keys necessary for decrypting the encrypted fob account identifier. Upon appropriate request from protocol/sequence controller 314, encryption/decryption component (e.g., circuitry 318) may retrieve the appropriate security key, decrypt the fob account identifier and forward the decrypted account identifier to protocol/sequence controller 314 in any format readable by any later connected POI terminal 110. In one

exemplary embodiment, the account identifier may be forwarded in a conventional magnetic stripe card format compatible with the ISO/IEC 7813 standard. That is, in accordance with the invention, there is no need to translate or correlate the account identifier to traditional magnetic stripe format as is done with the prior art. The invention processes the performance tracking transaction request directly, as if the card associated with the account has been presented for performance tracking.

[0085] Upon receiving the account identifier in magnetic stripe format, protocol/sequence controller 314 may forward the account identifier to POI terminal 110 via communications interface 312 and data link 122, as best shown in FIG. 1. Performance tracking terminal 110 may receive the decrypted account identifier and forward the magnetic stripe formatted account identifier to host network 112 for processing under the employer's business as usual standard. In this way, the present invention eliminates the need of a third-party server. Further, where POI terminal 110 receives a response from host network 112 (e.g., performance tracking authorized or denied), protocol/sequence controller 314 may provide the network response to RF module 302 for optically and/or audibly communicating

the response to fob 102 resource.

[0086] RFID reader 104 may additionally include USB interface 316, in communication with the protocol/sequence controller 314. In one embodiment, the USB interface may be a RS22 serial data interface. Alternatively, RFID reader 104 may include a serial interface such as, for example, a RS232 interface in communication with protocol/sequence controller 314. USB connector 316 may be in communication with a personalization system 116 (shown in FIG. 1B) for initializing RFID reader 104 to system 100 application parameters. That is, prior to operation of system 100, RFID reader 104 may be in communication with personalization system 116 for populating database 310 with a listing of security keys belonging to authorized fobs 102, and for populating database 320 with the security keys to decrypt fob 102 account identifiers placing the account identifiers in ISO/IEC 7813 format. In this way, RFID reader 104 may be populated with a unique identifier (e.g., serial number) which may be used by fob authentication circuitry 210 to determine if RFID reader 104 is authorized to receive fob 102 encrypted account identifier.

[0087] FIG. 1B illustrates an exemplary personalization system 100B, in accordance with the present invention. In gen-

eral, typical personalization system 100B may be any system for initializing RFID reader 104 and fob 102 for use in system 100A. With reference to FIG. 1B, the similar personalization process for fob 102 may be illustrated. For example, personalization system 116 may be in communication with fob 102 via RF ISO 14443 interface 114 for populating fob database 212 with the security keys for facilitating authentication of the unique RFID reader 104 identifier. In addition, personalization system 116 may populate on database 212 a unique fob 102 identifier for use by RFID reader 104 in determining whether fob 102 is authorized to access system 100. Personalization system 116 may populate (e.g., inject) the encrypted fob 102 account identifier into fob database 214 for later providing to an authenticated RFID reader 104.

[0088] In one exemplary embodiment, personalization system 116 may include any standard computing system as described above. For example, personalization system 116 may include a standard personal computer containing a hardware security module operable using any conventional graphic user interface. Prior to populating the security key information account identifier and unique identifying information into fob 102 or RFID reader 104, the

hardware security module may authenticate fob 102 and RFID reader 104 to verify that the components are authorized to receive the secure information.

[0089] In another exemplary embodiment, resource engine 130 may be configured to facilitate implementing the functions of personalization system 116. For example, resource engine 130 may be configured as personalization system 116. Thus resource engine 130 may be in communication with fob 102 via RF ISO 14443 interface 114 for populating fob database 212 with the security keys for facilitating authentication of the unique RFID reader 104 identifier. In addition, resource engine 130 may populate on database 212 a unique fob 102 identifier for use by RFID reader 104 in determining whether fob 102 is authorized to access system 100. Resource engine 130 may further populate (e.g., inject) the encrypted fob 102 account identifier into fob database 214 for later providing to an authenticated RFID reader 104.

[0090] FIGS. 6A–B illustrate an exemplary flowchart of a personalization procedure which may be used to personalize fob 102 and/or RFID reader 104. Although the following description discusses mainly personalization of fob 102, RFID reader 104 may be personalized using a similar pro-

cess. The personalization process, which occurs between personalization system 116 and the device to be personalized (e.g., fob 102 or RFID reader 104), may begin, for example at step 602. Mutual authentication may occur between personalization system 116 and the device to be authenticated in much the same manner as was described above with regard to fob 102 mutually authenticating with RFID reader 104. That is, personalization system 116 may transmit a personalization system 116 identifier to the device to be authenticated which is compared by the device authentication circuitry 210, 308 against personalization system identifiers stored in the device database 212, 310. Where a match does not occur (step 604), the personalization process may be aborted (step 612). Where a match occurs (step 604), personalization system 116 may prepare a personalization file to be provided to the device to be personalized (step 606). If personalization system 116 is operated manually, the personalization file may be entered into personalization system 116 using any suitable system interface such as, for example, a keyboard (step 606). Where personalization system 116 operator elects to delay the preparation of the personalization files, personalization system 116 may abort the personalization

process (step 610). In this context, the personalization file may include the unique fob 102 or RFID reader 104 identifier, security key for loading into database 212 and 310, and/or security keys for decrypting a fob transponder account identifier which may be loaded in database 320.

[0091] Fob 102 may be personalized by direct connection to personalization system 116 via RF ISO/IEC 14443 interface 114, or fob 102 may be personalized using RFID reader 104. Personalization system 116 and RFID reader 104 may engage in mutual authentication and RFID reader 104 may be configured to transmit the fob personalization file to fob 102 via RF. Once fob 102 is presented to RFID reader 104 (steps 608, 614) for personalization, fob 102 and RFID reader 104 may engage in mutual authentication (step 614). Where fob 102 is not presented to RFID reader 104 for personalization, the personalization process may be terminated (step 610).

[0092] If fob 102 is detected, personalization system 116 may create as a part of the personalization file, a unique identifier for providing to fob 102 (step 616). The identifier is unique in that one identifier may be given only to a single fob. That is, no other fob may have that same identifier. Fob 102 may then be configured and loaded with that

identifier (step 618).

[0093] The encrypted fob 102 transponder account identifier may be populated into fob 102 in the same manner as is described with respect to the unique fob 102 identifier. That is, personalization system 116 may pre-encrypt the account data (step 620) and inject the encrypted account into fob database 214 (step 622). The encrypted account data may be loaded (e.g., injected) into fob 102 using RFID reader 104 as discussed above.

[0094] Once the personalization file is populated into fob 102, the populated information is irreversibly locked to prevent alteration, unauthorized reading and/or unauthorized access (step 624). Personalization system 116 may then create a log of the personalization file information for later access and analysis by the personalization system 116 resource (step 626).

[0095] It should be noted that in the event the personalization process is compromised or interrupted (step 628), personalization system 116 may send a security alert to the resource (step 630) and the personalization process may be aborted (step 612). On the other hand, where no such compromising or interruption exists, personalization system 116 may be prepared to begin initialization on a sec-

ond device to be personalized (step 632).

[0096] FIGS. 7A–B illustrate another exemplary embodiment of a personalization process which may be used to personalize RFID reader 104. RFID reader 104 may be in communication with personalization system 116 via RFID reader USB connection 316 (step 702). Once connected, personalization system 116 may establish communications with RFID reader 104 and RFID reader 104 may provide personalization system 116 any RFID reader 104 identification data presently stored on RFID reader 104 (step 704). In accordance with step 708, where RFID reader 104 is being personalized for the first time (step 706), RFID reader 104 and personalization system 116 may engage in mutual authentication as described above with respect to FIGS. 6A–B. After the mutual authentication is complete, personalization system 116 may verify that RFID reader 104 is properly manufactured or configured to operate within system 100. The verification may include evaluating the operation of RFID reader 104 by determining if the RFID reader will accept predetermined default settings. That is, personalization system 116 may then provide RFID reader 104 a set of default settings (step 708) and determine if RFID reader 104 accepts those settings (step 712). If RFID

reader 104 does not accept the default settings, personalization system 116 may abort the personalization process (step 714).

[0097] If the personalization system 116 determines that the personalization process is not the first personalization process undertaken by RFID reader 104 (step 706), personalization system 116 and RFID reader 104 may engage in a mutual authentication process using the existing security keys already stored on RFID reader 104 (step 710). If authentication is unsuccessful (step 712), personalization system 116 may abort the personalization process (step 714).

[0098] Where personalization system 116 and RFID reader 104 successfully mutually authenticate, personalization system 116 may update RFID reader 104 security keys (step 716). Updating the security keys may take place at any time as determined by a system 100 manager. The updating may take place as part of a routine maintenance or merely to install current security key data. The updating may be performed by downloading firmware into RFID reader 104 (step 718). In the event that personalization system 116 determines in step 706 that RFID reader 104 is undergoing an initial personalization, the firmware may be loaded

into RFID reader 104 for the first time. In this context, "firmware" may include any file which enables the RFID reader 102 to operate under system 100 guidelines. For example, such guidelines may be directed toward the operation of RFID reader protocol/sequence controller 314.

[0099] Personalization system 116 may then determine if the personalization keys (e.g., security keys, decryption keys, RFID identifier) need to be updated or if RFID reader 104 needs to have an initial installation of the personalization keys (step 720). If so, then personalization system 116 may download the personalization keys as appropriate (step 722).

[0100] Personalization system 116 may then check RFID reader 104 to determine if fob 102 identifiers and corresponding security keys should be updated or initially loaded (step 724). If no updating is necessary personalization system 116 may end the personalization procedure (step 732). Contrarily, if personalization system 116 determines that fob 102 identifiers and corresponding keys need to be updated or installed, personalization system 116 may download the information onto RFID reader 104 (step 726). The information (e.g., fob security keys and identifiers) may be downloaded in an encrypted format and

RFID reader 104 may store the information in RFID reader database 310 as appropriate (step 728). Personalization system 116 may then create or update a status log cataloging for later use and analysis by personalization system 116 resource (step 730). Upon updating the status log, the personalization process may be terminated (step 732).

[0101] It should be noted that, in some instances it may be necessary to repersonalize the RFID reader in similar manner as described above. In that instance, the personalization process described in FIGS. 7A and 7B may be repeated.

[0102] FIG. 8 illustrates an exemplary flow diagram for the operation of system 100A. The operation may be understood with reference to FIG. 1A, which depicts the elements of system 100A which may be used in an exemplary transaction. The process is initiated when a resource desires to present fob 102 for performance tracking (step 802). Upon presentation of fob 102, the employer initiates the RF performance tracking transaction via RFID reader 104 (step 804). In particular, RFID reader 104 sends out an interrogation signal to scan for the presence of fob 102 (step 806). The RF signal may be provided via RFID reader antenna 106 or optionally via external antenna 108. The

resource then may present fob 102 for performance tracking (step 808) and fob 102 is activated by the RF interrogation signal provided.

[0103] Fob 102 and RFID reader 104 may then engage in mutual authentication (step 810). Where the mutual authentication is unsuccessful, an error message may be provided to the resource via the RFID optical and/or audible indicator (step 814) and the performance tracking transaction may be aborted (step 816). Where the mutual authentication is successful (step 814), a performance tracking request will be initiated. That is, RFID reader 104 may provide the resource with an appropriate optical and/or audible message (e.g., "performance tracking processing" or "wait") (step 818). Fob protocol/sequence controller 208 may then retrieve from database 214 an encrypted fob account identifier and provide the encrypted account identifier to RFID reader 104 (step 820).

[0104] RFID reader 104 may then decrypt the account identifier and convert the account identifier into magnetic stripe (ISO/IEC 7813) format (step 822) and provide the unencrypted account identifier to resource engine 130 (step 824). In particular, the account identifier may be provided to POI terminal 110 for transmission to host network 112

for processing (step 828). Processing performance tracking will be discussed in greater detail herein. Upon processing, POI terminal 110 may then send an optical and/or audible performance tracking status message to RFID reader 104 (step 830) for communication to the resource (step 832). Once the resource receives the status message, the transaction is completed (step 834.)

[0105] Processing performance tracking may be achieved by several methods. For example, in accordance with another aspect of the present invention, and with reference to FIG. 10, a resource 1002 may access resource engine 130 through user interface 118 to facilitate performance tracking, such as management, assignment, grading and/or scoring of resources, tasks, and/or applications.

[0106] More particularly, in one embodiment illustrated in FIG. 11, resource engine 130 may comprise a variety of subprograms and/or databases that facilitate managing, tracking, grading, and assigning resources, applications, skills, and tasks. Resource engine 130 may interface with various subprograms or databases, wherein the subprograms may be part of host network 112 and/or network 136. One skilled in the art will appreciate that resource engine 130 may additionally interface with components

directly, through a LAN network or indirectly via any other system or network.

[0107] The databases comprising resource engine 130 may be managed by an administrative resource 1160. Administrative resource may be an individual, software, and/or hardware configured to facilitate management, control, organization and/or oversight of resource engine 130. Additionally, there may be one or more parameters 1170 governing resource engine 130. Parameters 1170 may include, for example, security features, software requirements, hardware requirements, coding protocols and/or other requirements or preferences.

[0108] The databases comprising resource engine 130 may be interconnected such that information from one database may be accessed by one, two, three or more other databases. By the term "access," the databases may transmit, receive, obtain, link, connect, associate, interface, share, route, acquire, ascertain, retrieve, and gain information from one database to another. Thus, any information updated, received and/or sent to one database such as, for example, resource database 1130, may be automatically updated throughout all or any portion of the other databases that are accessed by resource database

1130.

[0109] For example, a resource database 1130 may access a master resource calendar 1180 for scheduling all resources. Master resource calendar 1180 may additionally access resource application calendar 1182 to access calendar and schedule information relating to the applications to which resource 1130 may be assigned. Resource database 1130 may also access a resource schedule 1132 for scheduling that specific resource. Additionally, resource database 1130 may access a resource skills database 1134 comprising information relating to the various skills of resource 1130. Resource database 1130 may access a resource application database 1154 comprising information relating to the application that resource 1130 is assigned to support. Further, resource database 1130 may access a resource application category 1136 comprising information relating to specific category subset of an application that a resource is assigned to support. Finally, resource database 1130 may access a manager database 1110 comprising information on managers and the portfolios for which the managers are responsible.

[0110] With further reference to an exemplary embodiment depicted in FIG. 2, application 1150 may also interface with

a plurality of databases. For example, a manager privilege class 1112 database may access application 1150 to obtain information regarding the queues of problem tickets assigned to various managers 1110. Resource applications 1154 may also access application 1150 in order to provide resource 1130 updates, changes and/or other information to application 1150. Application 1150 may further be accessed and divided into various sub-application categories 1152. Application categories 1152 may be further accessed by application category skills 1142 in order to determine what skills 1140 are needed to support application category 1152. Application categories 1152 may also be accessed by resource application categories 1136 in order to link resources 1130 to applications 1150.

[0111] With further reference to an exemplary embodiment illustrated in FIG. 11, task databases 1120 may also interface with a plurality of databases. For example, task 1120 may access resource application category 1136. Additionally, task 1120 may access an IMR database 1122, which may provide information on specific tasks associated with an IMR. Further, task 1120 may access databases such as a task class 1128, an estimated time of arrival (ETA) 1126, and a task day 1124 database. Task class 1128 may pro-

vide information on the classification of task 1120, for example, whether task 1120 is a build task. ETA 1126 may provide estimations on task 1120 completion times based on previous task completion times. Task day 1124 may provide scheduling information for task 1120 relating to when task 1124 was assigned and/or when it is scheduled to be completed.

[0112] While FIG. 11 illustrates a plurality of databases interfacing in a specific manner, any of the databases comprising resource engine 130 may interface to one another in any manner, and the interfaces or connections are not limited to those depicted. For example, task day 1124 may additionally access master resource calendar 1180 and/or any other database comprising resource engine 130.

[0113] In an exemplary embodiment, the databases within resource engine 130, as illustrated in FIG. 11, may operate in real-time. In this context, "real-time" includes information that may be immediately, or nearly immediately, accessed at the time an IMR and/or task is generated. For example, upon detection of an application problem, an IMR is generated. This IMR is then automatically broken down into applications and application tasks. The tasks are further automatically assigned to managers and/or re-

sources based on skill and availability. As such, upon discovery of an IMR, resource 1102 may immediately view or manage resources, applications, skills, and/or tasks associated with the IMR on resource engine 130 via user interface 118. Resource engine 130 may also immediately facilitate updates to resources, applications, skills, and/or tasks to a network such that resource 1102 may view any manual assignment or management changes through user interface 118.

[0114] One skilled in the art will also appreciate that resource engine 130 may operate fully or partially in any less than real-time mode, such as, for example, batch processing. In an exemplary embodiment, the system may operate partially in real-time and partially in batch mode, wherein during batch mode, system information may be stored, and periodically updated to the network. Thus, in this embodiment, resource 1102 may access resource engine 130 at a later time through user interface 118 to manage, assign, track, score or grade resources, tasks, applications, and skills.

[0115] The present invention may use the foregoing system components to perform the following method, wherein the exemplary steps discussed may be performed in any or

der. With respect to FIG. 12, resource 1102 may access resource engine 130 through user interface 118 (step 1201) by any communication method discussed herein. In one embodiment, resource 1102 selects a web-based option for interfacing with resource engine 130 such that the system presents the resource 1102 with an input screen. Resource engine 130 may then conduct an authorization (step 1203) by any method discussed herein, such as, for example, by use RFID reader 104 communicating with POI terminal 110.

[0116] Once authentication has occurred, resource engine 130 then may transmit a webpage and/or a resource screen for display on resource's 1102 computer (step 1205). The webpage and/or resource screen may facilitate access to resource engine 130 for performance tracking of resources (step 1207). With reference to an exemplary screen shot illustrated in FIG. 13, resource screen 1300 may be configured with one or more toolbars 1302 and/or task bars 1304 that facilitate navigation of engine 130. Toolbar 1302 may be configured to be visible to resource 1102 at all times when navigating engine 130 through user interface 118. Taskbar 1304 may be configured to facilitate performance tracking for the specific tool chosen

through toolbar 1302.

[0117] With continued reference to FIG. 13, resource screen 1300 may also be configured to facilitate resource 1102 using toolbar 1302 in selecting a variety of tools to be used by the present invention. These tools may include, for example, managing resources, IMRs, tasks, applications and skills through, for example, "ADMINISTRATION" 1311; viewing reports on resource tasks and skills, "REPORTS" 1313, automating and viewing task time, "TASK TIME" 1315; creating, assigning and updating tasks, "TASK MANAGEMENT" 1317; and/or creating resource rosters, schedules, and training "PLANNING" 1319. The details of these tools will be discussed below. In accordance with a further aspect of the present invention, one skilled in the art will appreciate that the web environment may be customizable and scalable, offering various other resource screen 1300 options depending upon the particular needs of resource 1102.

[0118] In accordance with the present invention, as illustrated in FIG's. 10, 12 and 13, resource 1102 may interact with resource engine 130 through user interface 118, using a device configured to facilitate interaction such as ADMINISTRATION 1311, available through resource screen 1300.

When accessing administration information through ADMINISTRATION 1311, resource 1102 may be presented with a variety of options regarding the information accessible through taskbar 1304. These may include, for example, "Manage Resources," "Manage Privilege Class," "Manage Application," and "Manage Skills." Each of these various categories may contain one or more additional links to further performance tracking.

[0119] The various resource fields may include, for example: First Name, Middle Name, Last Name, Phone Number, E-mail Address, Employer, Role, Manager, Location, Portfolio Description, Skill, Skill Level, Application, Resource Percentage, Start Date, and Weekly End Date. By selecting "Manage Resources," resource/manager 1002 may manage resources within its group by selecting the link/button indicating that specific task. By the terms "manage" and "management," resource/manager 1002 may add, edit, delete, save, assign, reassign, search, define, determine, create, and/or cancel information relating to resources within its group. For example resource/manager 1002 selecting the Edit button may make changes to various fields associated with a resource.

[0120] "Manage Resources" may be configured such that the only

time any of the Add, Edit, Delete, Save, or Cancel buttons will display is if the person trying to administer a resource has rights to do so. Thus, only a administrator, manager, manager/lead, and/or any other authorized person may update the Manage Resource screen. Resource engine 130 may be configured such that all buttons will be grayed out or un-selectable to resources 1002 without access rights.

[0121] After an authorized resource/manager 1002 inputs changes, resource engine 130 may be configured to present an error message if all required fields are not completed. If all required fields are completed, information inputted into the fields may be automatically updated into resource engine 130.

[0122] In accordance with an exemplary embodiment of the invention, fob resource 1002 may be provided limited access to a fob resource data file maintained within the "Manage Resources" area of resource engine 130 for managing the fob usage and fob resource 1002 information. Resource 1002 may have access over the phone, online, or off line. Resource 1002 may access the fob resource data file to change, for example, demographic information ((e.g. fob resource address, phone number, email address, or the like).

[0123] ADMINISTRATION 1311 may additionally facilitate the management of privilege classes through the "Manage Privilege Class" option on task bar 1304. Privilege classes may include designations, such as queue names, relating to IMRs/application failures tracked through resource engine 130 and/or through a monitoring program, such as NetView working in conjunction with resource engine 130. For example, NetView may automatically identify and generate a problem ticket describing the root cause of a network failure. NetView may then transmit the problem ticket/IMR to a specific network failure privilege class within resource engine 130. Transmission of the IMR from NetView to resource engine 130 may be through any communications means described herein.

[0124] By selecting "Manage Applications," resource/manager 1002 may manage applications and application categories. Additionally, resource/manager 1002 may assign/add resources to applications and/or application categories. Applications may be any software applications, processes, procedures, scripts, programs, and/or protocols running on a system. For example, Microsoft Word, a Service Delivery Platform application, and a windows application. Application categories may be any subsets of

Applications. For example, an Application may have a Distributive category and a Mainframe Category. By "assign" and/or "assignment," resource/manager 1002 may determine the resources to be assigned to applications, determine the resources to be assigned to application categories, define how much time a resource is assigned to an application or application category, determine the starting and/or ending date for an assignment for planning purposes, and/or track a resource's time spent on specific tasks, applications and/or application categories.

[0125] Additionally, resource/manager 1002 may use "ADMINISTRATION" 1311 to facilitate the management of resource skills by selecting the "Manage Skills" task. "Manage Skills" may be used to facilitate managing skills and skill sets available and/or needed for applications and application categories, defining and scoring the skills and skill sets of resources, determining skill set levels needed for application categories, assigning resources to application categories based upon resource skills and/or skill sets scores, determining skill set scores for resources assigned to those application categories, and redefining resource skills and/or skills set scores.

[0126] Resource engine 130 may employ one or more algorithms

to facilitate the management of resource skills. That is, one or more algorithms may be used in defining, scoring, determining, and assigning resources, skills, skills sets, and skill set needs. These algorithms may be automated such that resource engine 130 automatically tracks resources and application categories to continuously rescore and grade resource skills, skill sets and application categories. Resource engine 130 may also be configured to allow for manual calculation, scoring, and grading of resource skills, skill sets and application categories for assignment and management purposes.

[0127] Resource/manager 1002 may assign one or more skills to a specific category. For example, one application category (e.g. Service Delivery Platform services) may include multiple skills (a "skill set") to support it such as: Visual Basic, Microsoft SQL, exchange management skills, phone payment skills, information management skills, and Cobol. Resource/manager 1002 may additionally define "skill set" scores. For example, high Visual Basic, Microsoft SQL, and Cobol skills may be needed, while medium exchange management, and information management skills may be required and low phone payment skills may suffice. The skill set scores for the specific application category may

be as follows:

Skills	Skill Level	Score
Visual Basic	H	80
Microsoft SQL	H	80
exchange management	M	60
phone payment	L	30
information management	M	60
Cobol	H	80
Total		390

[0128] The application categories skills may be further scored to determine the score parameters for the skill levels needed

to support the category. For example, high skill levels would encompass scores that are 80% of 390 and above. An example of the parameters can be viewed in the following table:

80%	H	312
60%	M	234
30%	L	117

[0129] Resource engine 130 may be used to facilitate scoring skills and/or skill sets of resources. By "scoring," resource/manager 1002 defines a resource's skills for a specific category. The score levels may be, for example, high, medium, or low, wherein a high score may be assigned, for example, 80 points, a medium score may be assigned 60 points and a low score may be assigned 30 points.

[0130] For example, a resource's skills may be defined as follows:

Skills	Skill Level	Score
Visual Basic	M	60
Microsoft SQL	H	80
exchange management	L	30
phone payment	M	60
information management	L	30
Cobol	M	60
Total		320

[0131] The resource's skill set may be then compared to a category skill set to determine if the resource may be assigned to the category. This may be done by calculating a total resource category score based on the lower of the resource and task category scores. In the provided example, the resource's category skill score is 290. The resource therefore has medium-level category skills (where medium is any score from 234–311).

Resource Skill Score		Category Skill Score	Resource Category Score
60		80	60
80		80	80
30		60	30
60		30	30
30		60	30
60		80	60
Total	320	390	290
Category Level			M

[0132] Resource/manager 1002 may also use resource engine 130 to facilitate defining resource application portfolios. For example, resource engine 130 may be configured to gather all the application categories for a resource's portfolio of applications the resource is desired to support. Resource engine 130 may be configured to compute scores for the application categories in order to determine a rating for the resource, where the rating may range from a G1 (the lowest) to a G5 (the highest).

G-Rating	
G1	Greater than 0 but less than 75%
G2	Greater than or equal to 75% but less than 90%
G3	Greater than or equal to 90% but less than 110%
G4	Greater than or equal to 110% but less than 125%
G5	Greater than 125%
G-Rating	% of average standard hours

[0133] For example, a resource's application portfolio may contain three application categories. The resource may have ten different skills, each skill may be scored as follows:

Skills	Skill Level	Score
Skill-1	H	80
Skill-2	M	60
Skill-3	M	60
Skill-4	L	30
Skill-5	H	80
Skill-6	H	80
Skill-7	M	60
Skill-8	M	60
Skill-9	L	30
Skill-10	M	60

[0134] The three application categories in the resource's portfolio may have the following required skill sets:

Application Category 1		
Skills	Skill Level	Score
Skill-1	M	60
Skill-2	L	30
Skill-3	H	80
Skill-4	M	60
Skill-5	L	30
Total Score		260
80%	H	208
60%	M	156
30%	L	78

Application Category 2		
Skills	Skill Level	Score
Skill-2	M	60
Skill-6	L	30
Skill-7	H	80
Total Score		170
80%	H	136
60%	M	102
30%	L	51

Application Category 3		
Skills	Skill Level	Score
Skill-3	L	30
Skill-4	H	80
Skill-7	M	60
Skill-8	L	30
Total Score		200
80%	H	160
60%	M	120
30%	L	60

[0135] Thus, the resource will have a portfolio score as follows:

Res. Skills	Cat. Skills	Score	Res. Skills	Cat. Skills	Score	Res. Skills	Cat. Skills	Score
80	60	60	60	60	60	60	30	30
60	30	30	80	30	30	30	80	30
60	80	60	60	80	60	60	60	60
30	60	30				60	30	30
80	30	30						
Total		210	Total		150	Total		150
Level		H	Level		H	Level		M
Portfolio Total Score							510	

[0136] Resource engine 130 determines the rating of the resource based on the percentage of the total application category scores the resource scores in:

Application X	
Task	Total Score
Task-1	260
Task -2	170
Task -3	200
Total	630
1	<472.5
2	<567
3	<693
4	<787.5
5	>787.5

[0137] Thus, in order to achieve a G1 rating, the resource would need to score of less than 472.5. However, the resource in this example would rate as a G2 because the resource's

total portfolio score is 510, which is greater than the 75% range of the total category score of 630, but less than the 90% range.

[0138] Each portfolio may have its own defined scoring based on application categories that make up the portfolio. The selection process may be chosen by a manager and/or resource engine 130 which selects specific application categories for all applications the manager and/or resource engine 130 supports or by gathering all application categories for a specific resource.

[0139] In accordance with another aspect of the present invention, when hiring new hires, resource engine 130 may be configured to facilitate the generation of a portfolio application required for the new hire and a generation of a listing of skills that comprise the portfolio. Resource engine 130 may further be configured to facilitate grading of each skill based on interview answers and generating a total score and G rating for the potential new hire.

[0140] Further, resource engine 130 may be used to determine current resource skill levels in order to determine hiring needs, training needs, equipment, software, and/or hardware upgrades, and/or other needed support. Resource engine 130 may employ one or more algorithms to facili-

tate a determination of current resource skill levels. That is, one or more algorithms may be used in generating a portfolio application for a potential new hire, generating a listing of skills within the portfolio, grading the skills based on potential new hire answers, and generating a total score for the potential hire. These algorithms may be automated such that resource engine 130 automatically generates and grades potential new hire portfolios and interview. Resource engine 130 may also be configured to allow for manual generation of portfolios and portfolio skills and grading of potential hires.

[0141] With reference again to an exemplary embodiment depicted in FIG. 13, "TASK TIME" tool 1313 may be accessed by resource 1102 view automatically tracked time spent on different tasks. For example, resource 1102 may use fob 102 to communicate with RFID reader 104 when resource 1102 enters/leaves a work environment. Resource engine 130 may then calculate the total time resource 1102 was in the work environment by measuring the time between a first communication between fob 102 and RFID reader 104 and a second communication between fob 102 and RFID reader 104. For example, if a first communication occurs at 9:00 a.m. and a second communication oc-

curs at 5:00 p.m., then the time resource 1102 was in the work environment is eight hours. If resource 1102 enters and leaves a work environment multiple times throughout a reporting period (e.g., a day), resource engine may be configured to keep a running tally of times corresponding to each period between entering and leaving.

[0142] As used herein, the phrase work environment may include an office, a building, a shipping location, a computer environment, a computerized application, a computerized document, and/or any other work environment.

[0143] Resource engine 130 may be additionally configured to calculate the time between communications between fob 102 and interface 134 to determine the time spent by resource 1102 on specific tasks. For example, with reference to FIG. 1A, resource's 1102 may use fob 102 to automatically communicate with computer 134 when resource 1102 initiates use of computer 134. Computer 134 may be configured to log the tasks resource 1102 performs via computer 134. Computer 134 may also be configured to communicate information to resource engine 130 relating to the tasks resource 1102 performs via computer 134. Resource engine 130 may use this information to facilitate tracking the performance of resource

1102.

[0144] Resource engine 130 may also be configured to provide for "TASK MANAGEMENT" 1315 available through resource screen 1300. This tool may be used to facilitate management of application tasks. Tasks may include any project defined herein. Each task may be assigned to an application category and an application. Additionally, each task may have one or more subtasks with each subtask having a resource assigned to it. One manager may be assigned to each task.

[0145] Tasks may be further categorized by class. For example, tasks generated from problem tickets may be classified as IMRs. Other classes may include, for example, tasks relating to assembly, meetings, training, bridge calls, projects, analysis, design, programming and build tasks.

[0146] Resource engine 130 may also be used to facilitate the creation of subtasks associated with each task. For example, once an IMR is generated, subtask X may be the first task generated. Subtask X may relate to re-installing problem software. Additionally, another subtask for analyzing the re-installed software may be generated, subtask Y. An analyst resource may then review the re-installation and determine that another analysis and/or

installation task needs to be assigned. Resource engine 130 may be configured to automatically generate sub-tasks based on pre-programmed standards. For example, resource engine 130 may be pre-programmed to assign tasks relating to re-installation of software and analysis of a network whenever a network failure occurs. Resource engine 130 may also be configured for manual creation and/or reassignment of subtasks associated with each task.

[0147] Resource engine 130 may also be configured to automatically reassign a task and/or subtask to another resource if a resolution of the IMR has not been accomplished within a set task time period. For example, resource engine 130 may first assign IMR-related tasks of re-installation and analysis to be completed within 10 working hours. If the IMR has not been completed within a certain set time, such as, for example 15 hours, resource engine 130 may automatically reassign the re-installation and/or analysis tasks. Resource engine 130 may access time entries from "TASK TIME" to determine whether tasks have been completed within a predetermined time.

[0148] Resource engine 130 may also be configured to automatically generate a log of information relating to the re-

sources and tasks already completed and/or worked on relating to the IMR. For example, if Word, Excel and PowerPoint have already been reinstalled successfully, resource engine 130 may be configured to create a log of this information before reassigning the task.

[0149] Resource engine 130 may be configured to facilitate the grading of tasks as well. Tasks may also receive the same G-1 through G-5 ratings as resources. The ratings may be based on the actual hours taken to complete a task compared to a standard. The standard hours for a task may be defined by a lead programmer, a manager, and/or resource engine 130 using a model based on subjective standards for task completion times. The standard hours to complete a task may be based on the skill level of an average resource supporting an application. For resources with high skills, the standard hours may be 90% of the average standard hours. Similarly, for low skill resources, the standard hours may be 110% of the average standard hours.

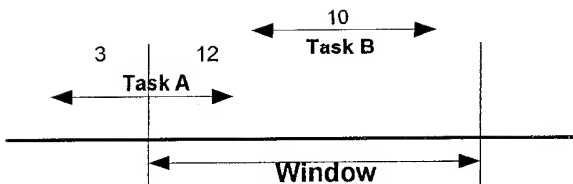
[0150] Ratings may be computed assuming the actual hours spent on a task. Errors may be created in labor tracking and often measuring a specific task may be inaccurate. However, resource engine 130 may increase accuracy by

combining the total effort for all tasks in a specified window of time. The bigger the window of time and/or the more tasks that are being graded, the more accurate the grading score.

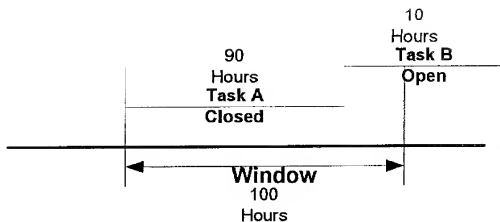
- [0151] For any chosen window, there may be the possibility of having open tasks and closed tasks. Resource engine 130 may be configured to grade only closed tasks. If a closed task falls partly within a window, it may be graded based on the percentage of the task within the window being graded. In order to determine this percentage, resource engine 130 may be configured to define a Factor to adjust the standard hours in the window. The Factor may be created as follows:

$$\text{Factor} = \frac{\text{Task Actual hours defined within window interval}}{\text{Total task Actual}}$$

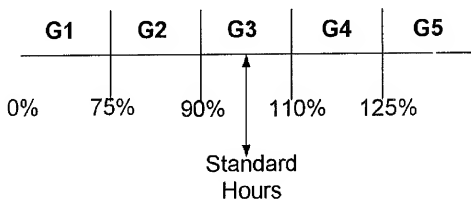
- [0152] Resource engine may be configured to multiply the Factor and the standard hours to determine the adjusted standard hours for a task. For example:



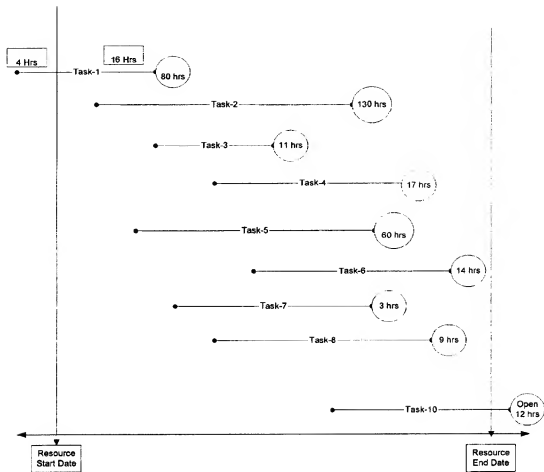
- [0153] Task B has 10 actual task hours and the hours are defined within the window Task B has a factor of 1 ($10/10 = 1$).
- [0154] Task A has 15 actual task hours, 12 hours are defined within the window, and 3 hours are outside of the window. Task A has a factor of .8 ($12/15 = 0.8$)
- [0155] Resource engine 130 may also be configured to grade the efficiency of tasks. In order to obtain a Grading efficiency for closed tasks, resource engine 130 may total all the closed tasks hours within a window and then divide that number by the sum of all task hours within the same window. The following example shows a window of 100 hours with 90 closed hours within the window.



[0156] The result is a grading efficiency of 90%. Based on a grading efficiency of 90, the G-rating would be G3.



[0157] The following is an example of how a resource task may be graded by resource engine 130. The diagram below illustrates 10 tasks assigned to a resource. It shows how the tasks relate to a window defined by the resource start and end dates.



[0158] The following chart shows that tasks 1 through 9 are closed and task 10 is still open. Resource engine 130 may use only the closed tasks for the grading. The total task hours equals 174 but only the closed task hours, equaling 166, may be used in the grading.

[0159] The chart also shows that task 1 has 20 actual hours but only 16 actual hours are inside of the window selected to grade. Resource Engine 130 may use a factor of 0.80 (16/20) to obtain the adjusted standard hours needed to

do grading. Tasks 2 through 9 are all within the window so their factor is equal to 1.00.

Actual Task Hours				
Task	Status	Task	Window	Factor
Task - 1	Closed	20	16	0.80
Task - 2	Closed	30	30	1.00
Task - 3	Closed	11	11	1.00
Task - 4	Closed	17	17	1.00
Task - 5	Closed	60	60	1.00
Task - 6	Closed	14	14	1.00
Task - 7	Closed	3	3	1.00
Task - 8	Closed	9	9	1.00
Task - 9	Closed	6	6	1.00
Task - 10	Open	12	8	
Total closed	task hours		166	
Total	task hours		174	

[0160] The next chart shows the application category assigned to the closed tasks and the standard hours associated with each application category. Resource engine 130 may be configured to multiply the standard hours against the factor to arrive at the adjusted standard hours. Resource engine 130 may additionally be configured to add the adjusted standard hours for all the closed tasks in order to obtain the total standard hours.

Application	Task	Standard Hours	Factor	Adjusted Standard Hours
Application Category 1	Task - 1	16	0.80	12.8
Application Category 1	Task - 2	32	1.00	32.0
Application Category 1	Task - 3	8	1.00	8.0
Application Category 1	Task - 4	16	1.00	16.0
Application Category 2	Task - 5	64	1.00	64.0
Application Category 2	Task - 6	16	1.00	16.0
Application Category 1	Task - 7	4	1.00	4.0
Application Category 1	Task - 8	8	1.00	8.0
Application Category 3	Task - 9	4	0.80	4.0
		Total Standard Hours		164.8

[0161] After resource engine 130 has determined the total standard hours, resource engine 130 can assign a grade and grade efficiency to the application category tasks. In the

example herein, the resource task grade would be G3 since 166 is under 181 and the Grade efficiency equals 95.4%.

	Standard Hours	164.8
	=	
Rating	Weight	Score
G1	75%	124
G2	90%	148
G3	110%	181
G4	125%	206
G5	Anything higher	

[0162] In accordance with an exemplary aspect of the present invention, resource engine 130 may be configured to facilitate assignment of tasks to resources. With reference to an exemplary flowchart illustrated in FIG. 14, a new IMR may be detected (step 1401) by resource engine 130 or by a software program such as NetView connected to resource engine 130. Resource engine 130 may then assign the IMR to an application category (step 1403). Resource engine 130 may use any method discussed herein for assigning to an application category. Resource engine 130 may then assign the IMR to a resource (step 1405) based upon the resource's skill. If the resource cannot do a task, resource engine 130 may reassign the task to a new resource.

[0163] Resource engine 130 may also generate a new task (step 1407) at the same time the new IMR is detected. Resource engine 130 may then assign/reassign the new task (step 1409) to a resource by any method discussed herein for assigning tasks. If the resource cannot do a task, resource engine 130 may reassign the task to a new resource.

[0164] Resource engine 130 may also be configured to determine whether scheduling allows for a resource to complete a task in a specific time level (step 1411). Resource engine

130 may access master calendars, master schedules, resource calendars, and/or resource schedules in order to determine optimum scheduling. If scheduling does not permit a resource to do a task within a time level, resource engine 130 may reassign the task to a new resource.

[0165] Once resource engine 130 has assigned a task to a resource whose schedule fits the correct time period, the resource may begin working the task to completion (step 1413). Resource engine 130 may also track (step 1415) the resource's work on the task to determine whether the resource has encountered problems with the task and needs additional help (step 1417). If resource engine 130 determines that the resource needs additional help, it may reassign the task to another resource (step 1409). If resource engine 130 determines that the resource does not need additional help, the resource will continue working the task to completion (step 1415).

[0166] With reference again to FIG. 13, "PLANNING" 1317 may be accessed within resource engine 130 to facilitate the creation of employee rosters, the scheduling of meetings, training, tasks, personal time and projects, and the calendaring of resources, tasks and projects. Resource/man-

ager 1002 may select create, manage, add, delete, update and/or define resource schedule hours per work week. Additionally, resource engine 130 may be used to facilitate the creation of a resource calendar of the schedules of all resource/manager's 1002 resources.

[0167] Resource/manager 1002 may also access resource engine 130 to facilitate the creation of a master resource calendar. A master resource calendar may include capacity hours, personal hours, and compensation hours. Capacity hours are the number of hours of planned capacity for a resource. For example, if a resource is scheduled to work eight hours per day each five-day work week, the capacity for the resource would be 40 hours. The Capacity hours may be recomputed monthly, weekly, daily and/or annually. Personal hours may be vacation time, sick time, visa constraint time, jury duty time, and/or any other type of time off of work. Personal hours may vary from one resource to another. Compensation hours may include time a resource is allowed to take off for overtime hours previously worked. Resource engine 130 may be configured to compute available hours based upon the Capacity hours minus Personal hours and Compensation hours.

[0168] Resource/manager 1002 may also access resource engine

130 to facilitate the management of a resource application calendar. A resource application calendar may store resource-specific information regarding the actual hours spent by a resource on an application, the number of hours planned for meetings and training, and whether a resource is working within its capacity. Resource engine 130 may connect the master resource calendar with a resource application calendar to best schedule resources and determine resource actualized hours.

[0169] Resource engine 130 may also be configured to provide for "REPORTS" 1319 available through resource screen 1300. This tool may be used to facilitate the generation of resource task and skill reports. The reports may be used by resource/manager 1002 to manage local and remote resources. For example, resource engine 130 may be used to generate reports on resource performance, resource capacities, resource training needs, resource skill sets, resource deficiencies, task performance, task resource needs, task skill set needs, and application performance. Additionally, resource/manager 1002 may use REPORTS 1319 to determine trends, problem areas, and efficiencies amongst resources, tasks, and applications. For example, resource/manager 1002 may access resource engine 130

to generate a report on various teams of resources to determine which teams work more effectively together and which teams under perform. Additionally, resource engine 130 may be used to facilitate a determination of hiring, training, and staffing needs.

[0170] In another exemplary application, illustrated in an exemplary embodiment depicted in FIG. 9, fob 102 may be configured to include a biometric security system 902, security system 902 may be used to facilitate performance tracking. In this case, a resource operating a fob may be asked to provide assurance that the resource is in fact the same resource whose details are stored on the fob. Accordingly, the resource may provide such verification by placing his finger over the biometric sensor 904. Biometric sensor 904 may then digitize the fingerprint and provide the digitized fingerprint for verification as described above. Once verified, fob 102 may provide a tracking transaction authorized signal to RF transponder 202 (or alternatively to transponder 220) for forwarding to RFID reader 104. RFID reader 104 may then provide the authorized signal to POI terminal 110 in a similar manner as is done with convention PIN driven systems and POI terminal 110 may process the transaction under the employer's

business as usual standard.

[0171] In another exemplary application, fob 102 and/or RFID reader 104 may be configured to facilitate biometric authentication of performance tracking. For example, a human resource using fob 102 and/or RFID reader 104 may pre-register biometric information that is unique to that human resource. For example, this biometric information may include one or more fingerprints, facial scans, retinal images, voice print, iris scans, and/or vascular patterns. By pre-registering, a user may set up one or more performance tracking accounts/tasks (e.g., programming tasks, build tasks, etc) associated with his biometric information. When a human resource desires to use fob 102 and/or RFID reader 104 to track his performance on a task, he may use a biometric security device, similar to that described herein, in association with fob 102 and/or RFID reader 104 for authentication purposes. By authentication, the human resource's present biometric information may be compared to the pre-registered biometric information to find a match. Once a match is made, the human resource may be authorized to choose one or more tasks associated with his biometric information in order to begin performance tracking.

[0172] In yet another exemplary application of the present invention, fob 102 may be configured for use with global positioning technologies. For example, fob 102 may include any combination of positioning technology such as global position system (GPS), wireless assisted GPS, wireless assisted protocol (WAP) based location, geography markoff language (GML) based location, differential GPS, enhanced observed time difference (E-OTD), enhanced cell identification, and uplink time difference of arrival (U-TDOA) technologies. Fob 102 may be configured to communicate its positional information to one or more servers on network 136 and/or resource engine 130 to provide information based on the location of fob 102. For example, a resource, such as a package, may be configured with a GPS-enabled fob 102 such that the package may be constantly tracked in order to monitor its delivery performance.

[0173] In accordance with another exemplary application of the present invention, fob 102 may be used for travel, shopping and/or other businesses to facilitate the tracking of travel, shopping and/or other activities. For example, a shopper resource carrying fob 102, may enter a store and use fob 102 to track his progress through the store. Further, different aisles and/or checkpoints throughout the

stores may be equipped with RFID readers 104 to facilitate tracking the shopper's performance. In a hardware store, as a further example, fob 102 may be used in conjunction with RFID readers 104 at the beginning and end of each aisle. Thus, when a shopper passes RFID reader 104, a performance tracking request may be initiated and recorded within resource engine 130. A manager and/or other user of resource engine 130 may then use this performance tracking data to determine which aisles the shoppers (and other shoppers) spend the most time in. The manager may then use this information to plan for scheduling employees, stocking supplies, ordering products, and/or any other related tasks. As yet another example, museums may use fobs 102 and RFID readers 104 to track wait times, viewing times, heavily trafficked areas and other related matters.

[0174] In another embodiment of the present invention, fob 102 may be used on all products in a business, such as, for example, a grocery store. The store may have various RFID readers 104 equipped throughout, such that managers and/or other users may track the different products throughout the store for security, stocking and/or other purposes. For example, RFID reader 104 may be used in

conjunction with one or more third-party merchant systems, as described more fully in U.S. Patent Application No. 10/192,488, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS." Third-party merchant systems may include any issuer system and/or merchant system maintained by an entity, such as, for example a non-financial or financial institution, American Express®, Visa® and/or MasterCard®, etc.

[0175] As an example of an exemplary aspect of the present invention in conjunction with the merchant system, fobs 102 and RFID reader 104 may be configured to eliminate the need for a clerk during checkout. Fobs 102 and RFID reader 104 may also facilitate transaction time for shoppers. For example, a shopper may push his cart past RFID reader 104 and all the products in the cart may communicate purchasing information to RFID reader 104 and one or more third-party merchant system via fobs 102 affixed to the products. A third-party merchant system may then be used to execute a payment transaction for the products. The shopper may then perform the transaction in an expedited way, as neither the ringing up of the products nor payment for the products may require a clerk's assis-

tance. Additionally, RFID reader 104 may be configured to communicate product and purchasing information relating to the transaction to resource engine 130 for tracking purposes.

[0176] While security measures exist that allow stores to monitor whether products have been shoplifted, these security measures must be removed and/or deactivated at check-out. As a further example of an exemplary aspect of the present invention, fobs 102 may be configured such that they do not require deactivation and/or removal. Instead, fobs 102 and RFID reader 104, used in conjunction with products, may be configured to communicate with one or more third-party merchants and resource engine 130 to track the purchasing status of the products. For example, resource engine 130 may be configured to track whether fob 102 and RFID reader 104 have been used to engage in a merchant transaction. Thus, if a shoplifter tries to leave a store without paying for a product, RFID reader 104, located at the exit of the store, may be configured to communicate with resource engine 130 in order to determine whether the product was the subject of a merchant transaction. If resource engine 130 indicates that the product was not the subject of a merchant transaction, RFID reader

may be configured to sound an audible and/or silent alarm and/or communicate with an alarm system to alert the store's security personnel.

[0177] The preceding detailed description of exemplary embodiments of the invention makes reference to the accompanying drawings, which show the exemplary embodiment by way of illustration. While these exemplary embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the invention. For example, the steps recited in any of the method or process claims may be executed in any order and are not limited to the order presented. Further, the present invention may be practiced using one or more servers, as necessary. Thus, the preceding detailed description is presented for purposes of illustration only and not of limitation, and the scope of the invention is defined by the preceding description, and with respect to the attached claims.

[0178] Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions

to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of any or all the claims. As used herein, the terms "comprises," "comprising," or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Further, no element described herein is required for the practice of the invention unless expressly described as "essential" or "critical."